SafeAudio Peak + 2

(12) UK Patent Application (19) GB (11) 2 382 670 (13) A

(43) Date of A Publication 04.06.2003

(21) Application No 0118161.9

(22) Date of Filing 25.07.2001

(71) Applicant(s)
Macrovision Corporation
(Incorporated in USA - Delaware)
2830 De La Cruz Boulevard, Santa Clara, California 95050, United States of America

(72) Inventor(s)
Adrian Robin Aylward
Richard A. A. Heylen

(74) Agent and/or Address for Service
W H Beck, Greener & Co
7 Stone Buildings, Lincoln's Inn, LONDON, WC2A 3SZ, United Kingdom

(51) INT CL[7]
G06F 12/14

(52) UK CL (Edition V)
G4A AAP A23X
G5R RB265 RHB

(56) Documents Cited
GB 2377511 A **GB 2371916 A**
EP 1271511 A2 **WO 2001/015028 A1**

(58) Field of Search
UK CL (Edition V) **G4A AAP, G5R RHB**
INT CL[7] **G06F 1/00 12/14**
Other: **ONLINE: WPI, EPODOC, JAPIO, TDB, INSPEC**

(54) Abstract Title

A method of copy protection of digital data by altering codewords to introduce impulse errors which are then marked as uncorrectable

(57) A digital audio compact disc is copy protected by introducing altered values into the encoded digital audio data. In addition, all of the codewords containing the introduced altered values are changed so that the altered codewords are identified as uncorrectable. This identification of codewords as uncorrectable is used to force the altered data values to be subject to interpolation or other concealment means during playback of the audio data. As a data reader does not utilise error concealment means when reading data it may subject the altered codewords to additional attempts at correction or may pass the digital audio data, incorporating the altered values, unchanged. This means that if a data reader is used as the input to a copier, the copy produced will be degraded. In this respect, the altered values correspond to impulses (82, Fig 8a) superimposed onto the analog audio data (80) and are audible as clicks.

Preferably the altered values are positioned so as to correspond to the particular features in the analogue audio waveform. Such features may be peaks, to maximise the loudness of the clicks produced by the introduced impulse. Alternatively the altered values can be placed to correspond to other areas in which the rate of change (gradient) of the waveform is low; or, simply at specific places chosen by reference to waveform shape. Other preferable features include the XOR-ing of at least four bytes of codewords with a value of at least four bytes and changing only parity bytes of a codeword.

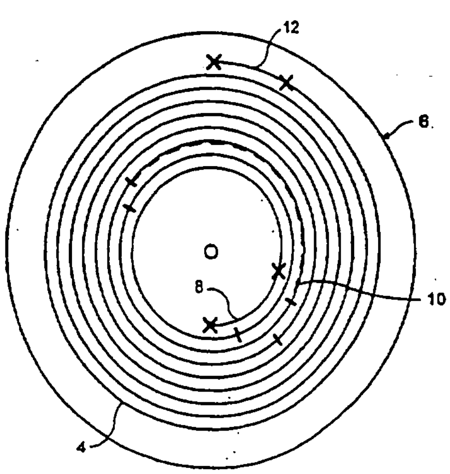


FIG.1

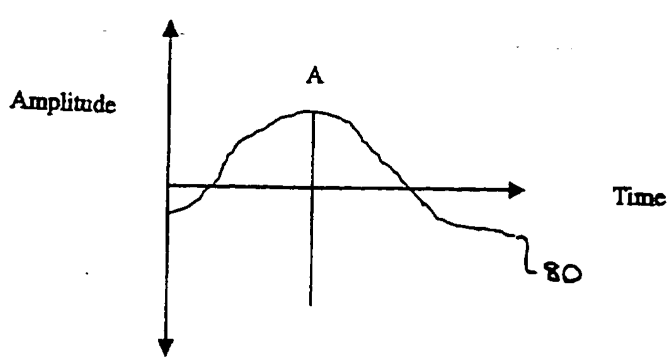


Figure 8b

GB 2 382 670

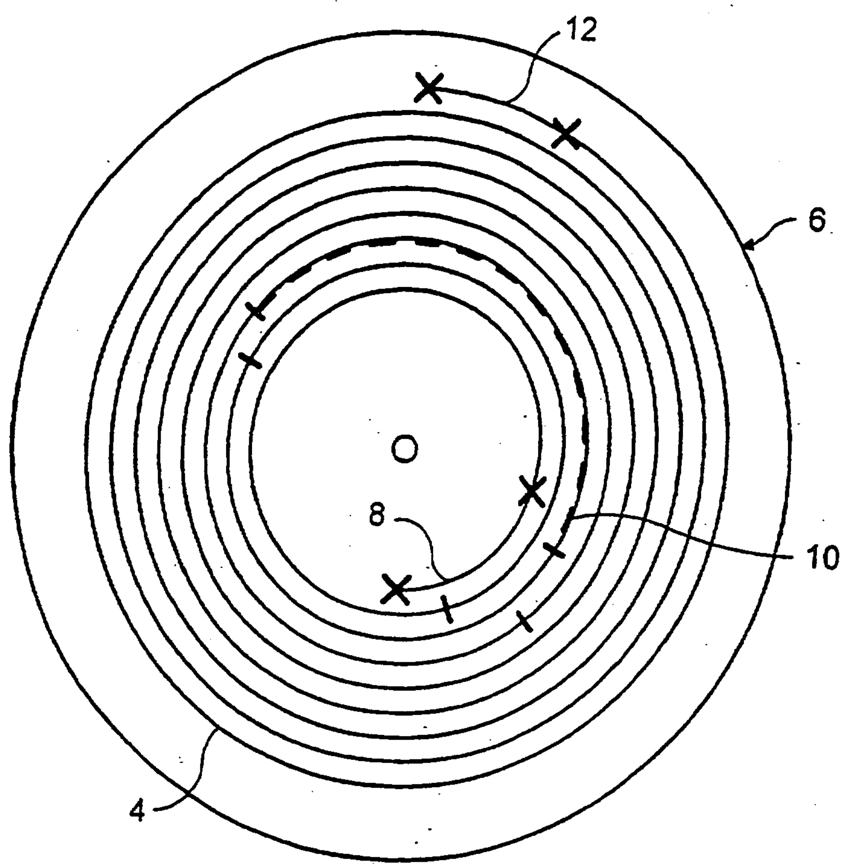


FIG.1

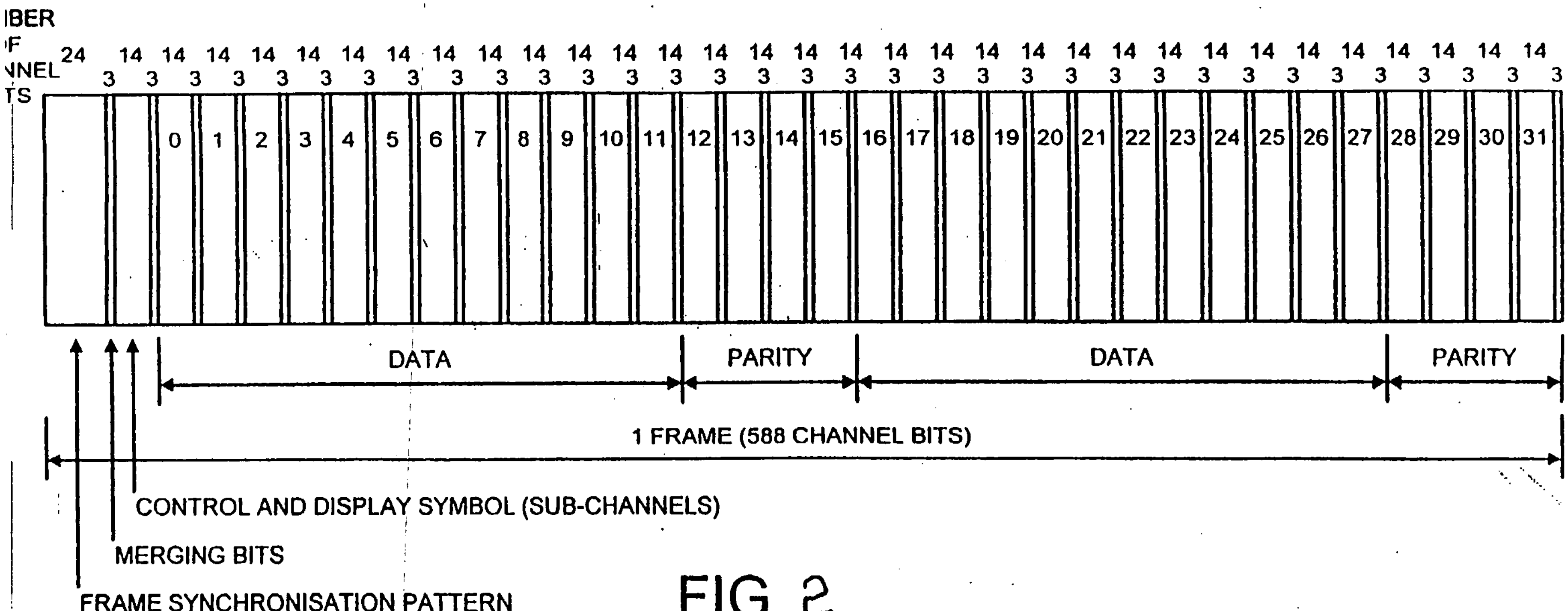

IBER
F
NNEL
TS
24
14
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
DATA
PARITY
DATA
PARITY
1 FRAME (588 CHANNEL BITS)
CONTROL AND DISPLAY SYMBOL (SUB-CHANNELS)
MERGING BITS
FRAME SYNCHRONISATION PATTERN

FIG. 2

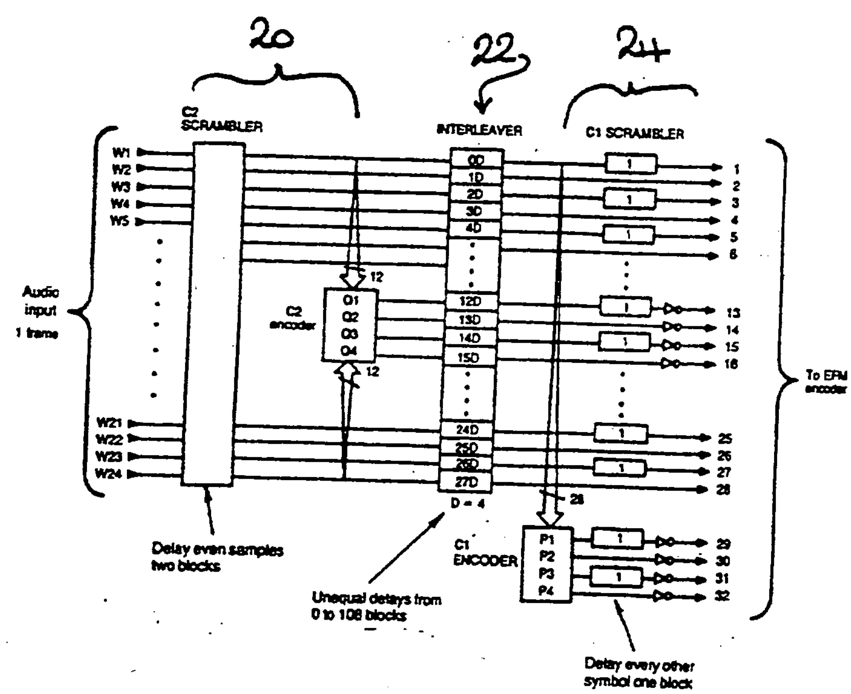

20
22
24
C2 SCRAMBLER
INTERLEAVER
C1 SCRAMBLER
W1
W2
W3
W4
W5
W21
W22
W23
W24
Audio input
1 frame
C2 encoder
Q1
Q2
Q3
Q4
12
0D
1D
2D
3D
4D
12D
13D
14D
15D
24D
25D
26D
27D
D = 4
C1 ENCODER
P1
P2
P3
P4
28
To EFM encoder
Delay even samples two blocks
Unequal delays from 0 to 108 blocks
Delay every other symbol one block

Figure 3

		C2								
	26	S0	S1	S2	Q0	S3	S4	S5	P0	
		S6	S7	S8	Q1	S9	S10	S11	P1	
C1		S12	S13	S14	Q2	S15	S16	S17	P2	28
C1		S18	S19	S20	Q3	S21	S22	S23	P3	28
		S24	S25	S26	Q4	S27	S28	S29	P4	
		S30	S31	S32	Q5	S33	S34	S35	P5	
		S36	S37	S38	Q6	S39	S40	S41	P6	
		S42	S43	S44	Q7	S45	S46	S47	P7	
		S48	S49	S50	Q8	S51	S52	S53	P8	

Figure 4

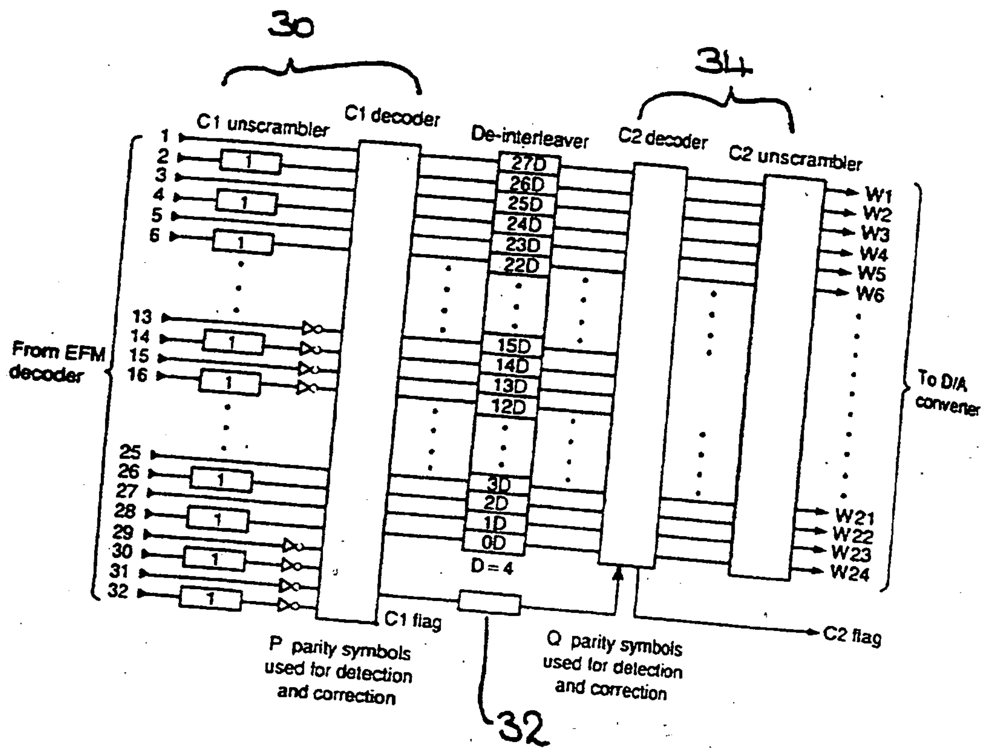

30
34
C1 unscrambler
C1 decoder
De-interleaver
C2 decoder
C2 unscrambler
From EFM decoder
To D/A converter
27D
26D
25D
24D
23D
22D
15D
14D
13D
12D
3D
2D
1D
0D
D = 4
W1
W2
W3
W4
W5
W6
W21
W22
W23
W24
C1 flag
C2 flag
P parity symbols used for detection and correction
Q parity symbols used for detection and correction
32

Figure 5

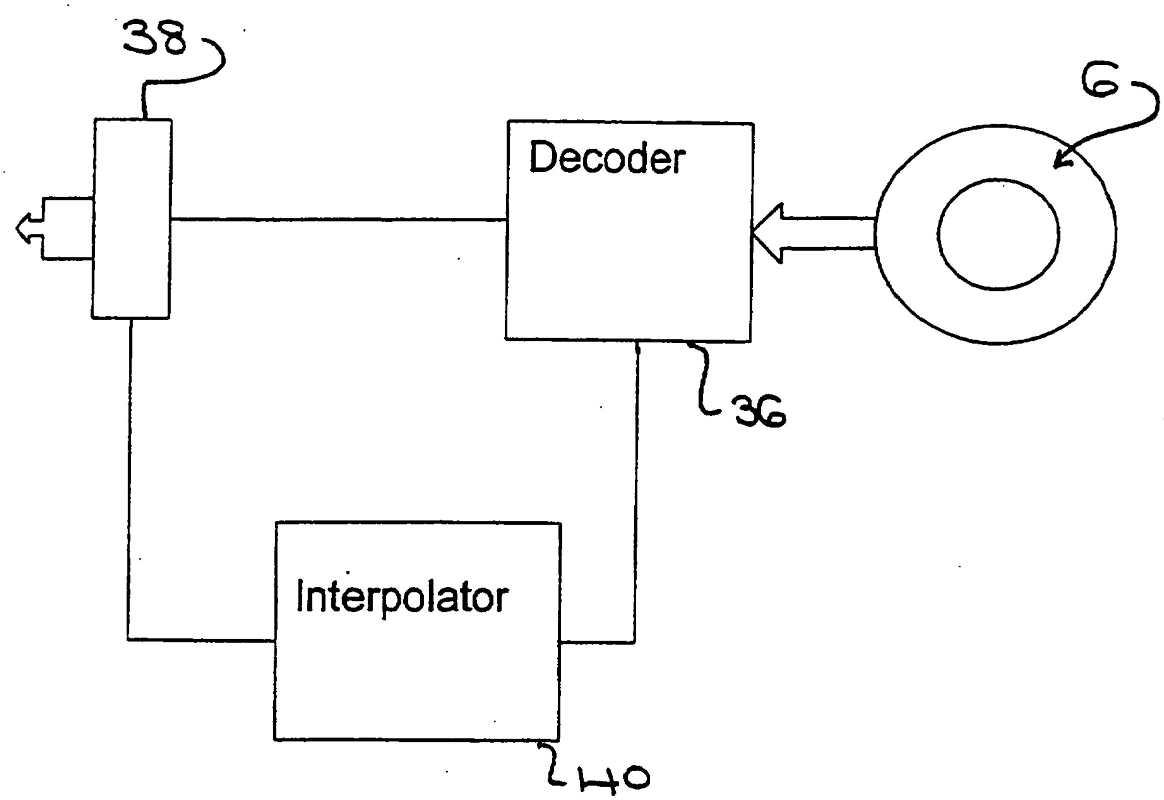


Figure 6

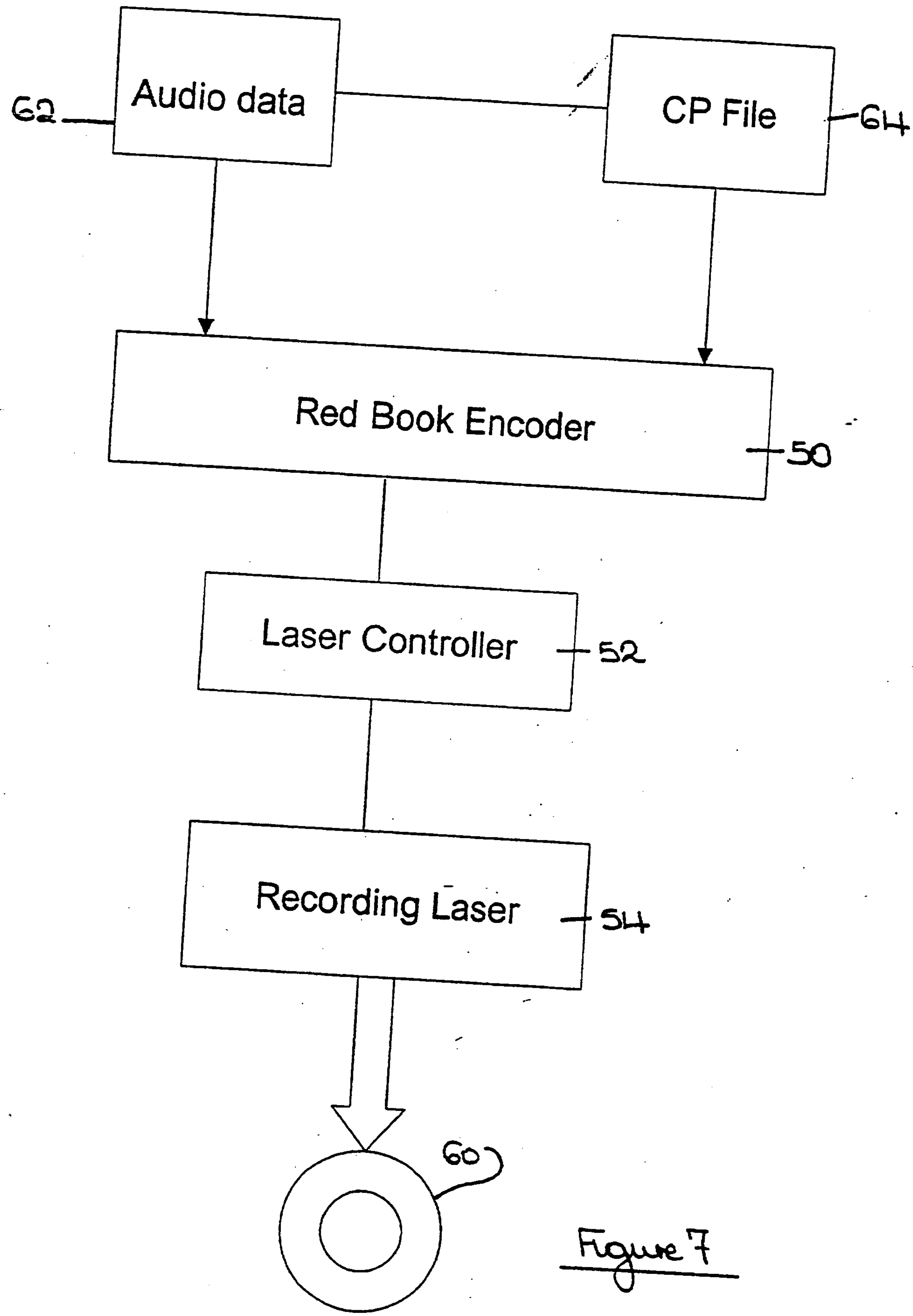

Audio data
62
CP File
64
Red Book Encoder
50
Laser Controller
52
Recording Laser
54
60

Figure 7

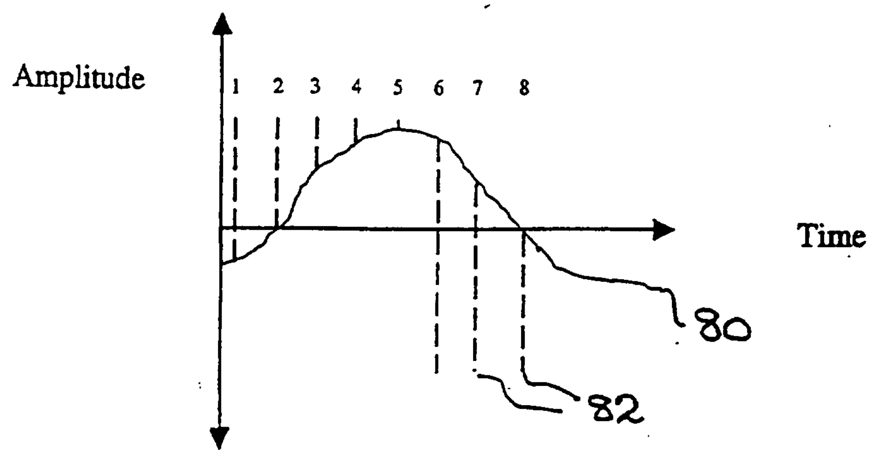


Figure 8a

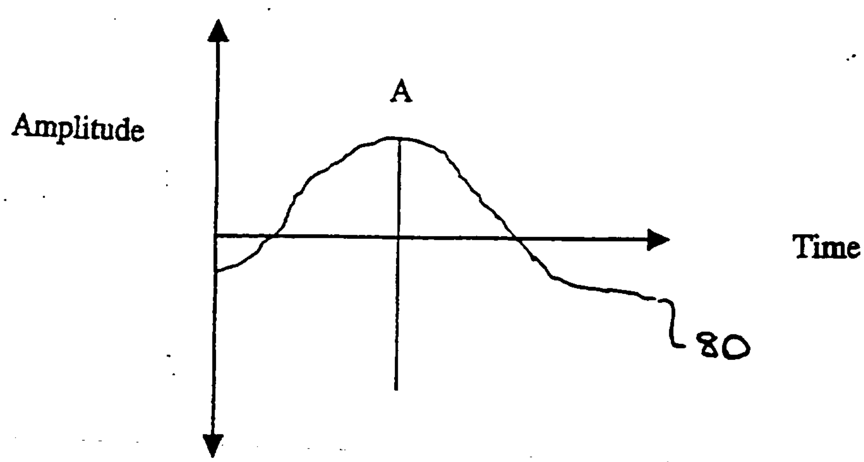


Figure 8b

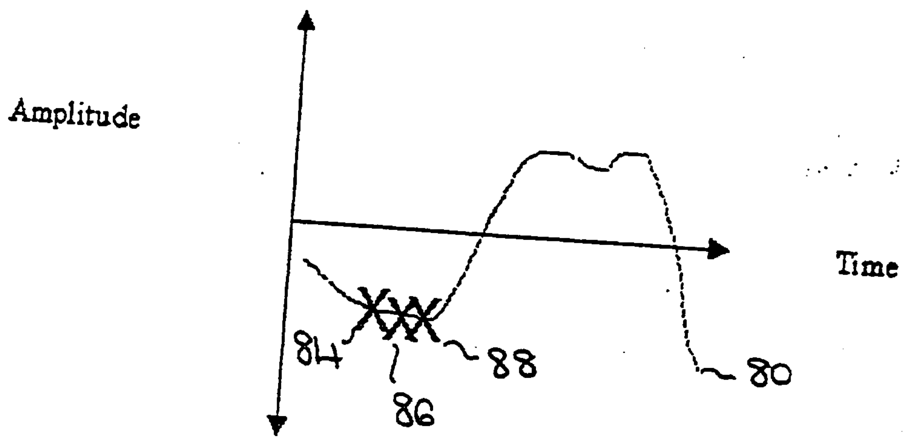


Figure 9

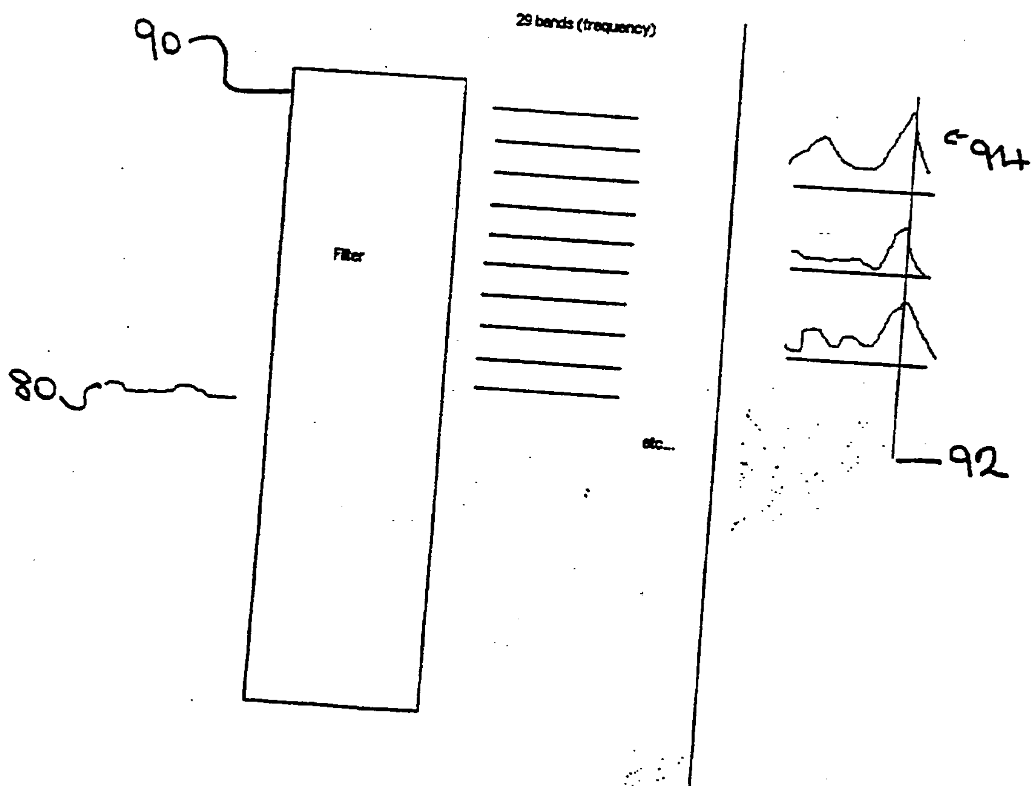


Figure 10

2382670

THE COPY PROTECTION OF DIGITAL AUDIO DATA

The present invention relates to a method of copy protecting digital audio data and to copy protected media on which the digital audio data is stored.

Digital audio compact discs (CD-DA) which carry music or other audio can be played or read by more sophisticated apparatus, such as CD-ROM drives. This means, for example, that the data on a CD-DA acquired by a user may be read into a PC by way of its ROM drive and thus copied onto another disc or other recording medium. The increasing availability of recorders able to write to CDs is therefore an enormous threat to the music industry.

In an earlier proposed method, a digital audio compact disc is copy protected by rendering control data encoded onto the disc incorrect and/or inaccurate. The incorrect data encoded onto the CD is either inaccessible to, or not generally used by, a CD-DA player. Therefore, a legitimate audio CD bought by a user can be played normally on a compact disc music player. However, the incorrect data renders the CD unplayable by a CD-ROM drive.

However, as the audio compact disc is rendered unplayable on a CD-ROM drive, the user is also prevented from using the CD-ROM drive legitimately simply to play the music or other audio on the disc.

What is needed is a method of copy protection for a digital audio compact disc which, whilst preventing the production of usable copy discs, does not prevent or degrade the playing of protected audio discs on all players having the functionality to play audio discs.

WO 01/15028 discloses a method of copy protecting a CD-DA in which errors are introduced into the audio data itself. These errors are to be identified as 'uncorrectable' by the error correction arrangements normally provided in audio players or data readers. As a result, an audio player will conceal the errors, for example by substituting interpolated values for audio data identified as erroneous, whereas a data reader will either fail to read the erroneous data or will simply read the erroneous values. The uncorrectable errors on the CD-

DA will, therefore, either render the protected CD-DA uncopiable, or they will add unacceptable noise when a copy of the protected CD-DA is played.

An improved copy protection scheme of the type described in WO 01/15028 is described in our co-pending British patent application No. 0116278.3.

The present invention is concerned with alterations which may be made to the audio data to be copy protected by methods as described in the two earlier applications referred to above.

According to a first aspect of the present invention there is provided a method of copy protecting encoded, digital, audio data, the method comprising the steps of:

introducing altered values into the encoded digital audio data, and

changing all codewords containing the introduced altered values such that, on decoding, the codewords can be identified as uncorrectable,

wherein said altered values correspond to impulses superimposed onto the analog audio data, each said superimposed impulse being located at or near a peak in the analog audio waveform.

In a method of an embodiment of the invention, the location of superimposed impulses at or near existing peaks in the audio waveform maximises the audible clicks which result from the superimposed impulses.

Preferably, the impulses superimposed onto the analog audio data each have a polarity which is opposite to the polarity of the peak at or near which the superimposed impulse is located.

The provision of superimposed impulses of opposite polarities to those of the respective peaks ensures that the resulting clicks are more readily discernible to the human ear.

The codewords may be changed by modifying elements of the appropriate codewords as described either in British application No. 0116278.3 or in WO 01/15028.

In a preferred embodiment, at least four bytes of each codeword are changed by XOR with a value of four or more bytes. Preferably, all bytes changed are parity values.

The copy protection method of the invention is arranged to identify codewords with altered values as uncorrectable. The audio player would generally be provided with error concealment means such as an interpolator. The identification, therefore, of codewords as uncorrectable is used to force the altered data values to be subject to interpolation or other concealment means during playback of the audio data.

However, a data reader does not utilise error concealment means when reading data, although it may use further decoding and error correction means to try to further correct the data. If, therefore, the encoded and copy protected digital audio data produced by a method of the invention is decoded by a digital reader and is flagged as uncorrectable, the audio data may be subject to additional attempts at correction and/or then the digital audio data, incorporating the altered values, is passed unchanged. If the data reader is being used as the input to a copier, for example, the altered values will be encoded onto the copy medium, such as a CD-DA. By this means, the copy produced will be degraded.

In a preferred embodiment of the invention, the altered values are introduced by identifying peaks in the analog audio data and superimposing impulses on the analog audio data prior to its encoding.

Alternatively, the altered values are made in digital audio data at locations identified as peaks in the analog audio data.

In a preferred embodiment of a method as defined above, additional altered values correspond to impulses superimposed onto the analog audio data, each said additional superimposed impulse being located in the analog audio data where the audio waveform has a slow or steady rate of change.

Where the audio waveform has a slow or steady rate of change, the audio data values calculated by an interpolator during playback are likely to be

a good approximation such that there will be little degradation of the reproduced sound.

According to a further aspect of the present invention there is provided a method of copy protecting encoded, digital, audio data, the method comprising the steps of:

introducing altered values into the encoded digital audio data, and

changing all codewords containing the introduced altered values such that, on decoding, the codewords can be identified as uncorrectable,

wherein said altered values correspond to impulses superimposed onto the analog audio data, each said superimposed impulse being located in the analog audio waveform where that audio waveform has a slow or steady rate of change.

In a preferred embodiment, an area in the analog audio waveform is located where there are at least three successive audio values arranged substantially in a straight line, and the superimposed impulse is located at a middle one of the three successive values.

It has been found to be possible to hide a sound in audio, or to enhance that sound, by the use of time masking and frequency masking techniques. It is also possible to calculate from filtered frequency bands, for example, whether the human ear can discern a click. Such techniques can be used with a copy protection method of the invention to hide superimposed impulses to ensure less degradation of the audio reproduced by an audio player. Alternatively, these techniques can be used to enhance the effect of superimposed impulses to improve the effectiveness of the copy protection.

In a preferred embodiment, further additional altered values are introduced into the encoded digital audio data, said further additional altered values corresponding to impulses superimposed onto the analog audio waveform, the position of each said superimposed impulse being chosen after determining by time masking or frequency masking techniques whether or not it can be heard by the human ear.

Superimposed impulses from said further additional altered values can be located either where they are masked from the human ear or where their effect is enhanced to the human ear.

According to a still further aspect of the present invention there is provided a method of copy protecting encoded, digital, audio data, the method comprising the steps of:

introducing altered values into the encoded digital audio data, and

changing all codewords containing the introduced altered values such that, on decoding, the codewords can be identified as uncorrectable,

wherein said altered values correspond to impulses superimposed onto the analog audio waveform, each said superimposed impulse being located in the analog audio waveform as determined by frequency or time masking techniques.

The present invention also extends to a medium on which copy protected encoded digital audio data has been stored, wherein the medium carries digital audio data into which altered values have been introduced, and codewords, containing the introduced altered values, which have been changed such that they will be identified as uncorrectable on decoding, wherein said altered values correspond to impulses superimposed onto the analog audio data, the location of said superimposed impulses having been chosen by reference to the shape of the analog audio waveform.

The present invention also extends to a copy protection file arranged to alter digital audio data, and codewords produced therefrom, by methods as defined above.

Embodiments of the present invention will hereinafter be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows schematically a CD,

Figure 2 shows the format of a frame of data on a CD,

Figure 3 shows schematically a CIRC encoder for data to be encoded on to a CD,

Figure 4 shows a block of data after encoding,

Figure 5 shows a CIRC decoder,

Figure 6 shows schematically an audio player, and

Figure 7 shows a circuit for applying a copy protection scheme of the invention to a CD,

Figures 8a and 8b show an audio waveform, Figure 8a illustrating the effect of location on the loudness of superimposed impulses, and Figure 8b illustrating the superimposing of an impulse at a peak of the waveform,

Figure 9 shows the choice of the location of a superimposed impulse to provide for control of its effect, and

Figure 10 illustrates filtering techniques used to mask or enhance superimposed impulses.

The practice of encoding digital data was developed to ensure that the correct information was received over early communications channels, such as the telegraph, despite noise. Now, however, digital data is routinely encoded to allow any errors in the data to be detected and corrected. In this respect, the basic methods of the invention described herein are described with particular reference to the encoding and decoding of audio data on CD-DAs. However, it will be appreciated that these methods are equally applicable in any context where there is digital audio data which is to be encoded, for example, for reliability, and where errors in the digital audio data are to be concealed, on playback, by interpolation or other error concealment techniques.

We will look briefly at the encoding of digital data on CD-DAs and at the copy protection schemes described in WO 01/15028 and GB0116278.3.

A digital audio compact disc (CD-DA), which carries music and is to be played on an audio player such as a conventional CD disc player, is made and recorded to a standard format known as the *Red Book* standards. As well as defining physical properties of the disc, such as its dimensions, and its optical properties, such as the laser wavelength, the *Red Book* also defines the signal format and the data encoding to be used.

As is well known, the use of the *Red Book* standards ensure that any CD-DA produced to those standards will play on any audio player produced to those standards.

Figure 1 shows schematically the spiral track 4 on a CD 6. This spiral track 4 on a CD-DA is divided into a Lead-In 8, a number of successive music or audio tracks as 10, and a Lead-Out 12. The Lead-In track 8 includes a Table of Contents (TOC) which identifies for the player the tracks to follow, whilst the Lead-Out 12 gives notice that the spiral track 4 is to end.

An audio player always accesses the Lead-In track 8 on start up. The music tracks may then be played consecutively as the read head follows the track 4 from Lead-In to Lead-Out. Alternatively, the player navigates the read head to the beginning of each audio track 10 as required.

To the naked eye, a CD-ROM looks exactly the same as a CD-DA and has the same spiral track 4 divided into sectors. However, data readers, such as CD-ROM drives, are enabled to read data, and process information, from each sector of the compact disc according to the nature of that data or information. A data reader can navigate by reading information from each sector whereby the read head can be driven to access any appropriate part of the spiral track 4 as required.

To ensure that any data reader can read any CD-Rom, the compact discs and readers are also made to standards known, in this case, as the *Yellow Book* standards. These *Yellow Book* standards incorporate, but extend, the *Red Book* standards. Hence, a data reader, such as a CD-ROM drive, can be controlled to play a CD-DA.

The ability of a data reader to access, extract, or otherwise read the data on a CD-DA provides a problem for the music industry. A user can use his CD-ROM drive to read the data from an audio disc, for example, into a computer file, and then that data can be copied. The increasing availability of recorders able to record onto compact discs means that individuals and organisations now have easy access to technology for making perfect copies of audio compact discs. This is of great concern to the music industry.

As the data encoding on a CD-DA and on a CD-ROM is well known and in accordance with the appropriate standards, it is not necessary to describe it in detail herein.

Briefly, the data on a CD is encoded into frames by EFM (eight to fourteen modulation). Figure 2 shows the format of a frame, and as is apparent therefrom, each frame has sync data, sub-code bits providing control and display symbols, data bits and parity bits. Each frame includes 24 bytes of data, which, for a CD-DA, is audio data.

There are 8 sub-code bits contained in every frame and designated as P, Q, R, S, T, U, V and W. Generally only the P and Q sub-code bits are used in the audio format. The standard requires that 98 of the frames of Figure 3 are grouped into a sector, and the sub-code bits from the 98 frames are collected to form sub-code blocks. That is, each sub-code block is constructed a byte at a time from 98 successive frames. In this way, 8 different subchannels, P to W, are formed. These subchannels contain control data for the disc. The P- and Q- subchannels incorporate timing and navigation data for the tracks on the disc, and generally are the only subchannels utilised on an audio disc.

Before the data on a CD is subjected to EFM encoding and formed into the frame structure illustrated in Figure 2, it is subjected to error correcting encoding. Specifically, the data to be stored on a CD is interleaved to distribute errors, and has parity values incorporated for error correction. The particular algorithm used in the compact disc system is the Cross Interleave Reed-Solomon Code (CIRC) and an example of the CIRC encoding scheme is shown in Figure 3. As can be seen, a C2 encoder 20 accepts 24 bytes of audio data, subjects some bytes to delay, and produces four bytes of Q parity values. Cross interleaving by way of an interleaver 22 follows the C2 encoder 20 whereby the 28 bytes are delayed by different periods. As a result of this interleaving, each C2 word is stored in 28 different C1 codewords.

A C1 encoder 24 accepts a 28 byte vector containing data from 28 different C2 codewords, and produces 4 more bytes of P parity values. The resulting 32 byte codewords leave the CIRC encoder of Figure 3 and are applied to the EFM encoder.

An example of a block of data produced by a CIRC encoder of Figure 3 is illustrated in Figure 4 where each S value represents 4 bytes of data, each Q value represents 4 bytes of Q parity values, and each P value represents 4

bytes of P parity values. In addition, Figure 4 illustrates the data rows, as 26, which are subject to decoding by a C2 decoder, and the data rows, as 28, which are subject to decoding by a C1 decoder.

Figure 5 shows schematically a CIRC decoder for decoding blocks of data from a CD. Thus, and as is known, the pits and lands on a CD are read and subject to EFM demodulation and are then applied to the CIRC decoder for de-interleaving, error detection and error correction. The data is input to the decoder in blocks as shown in Figure 4 and is output as 24 bytes of audio data.

Thus, a frame of 32 8 bit words are applied to the decoder of Figure 5. This frame of 32 bytes includes 24 bytes of audio data and 8 bytes of parity values. In a C1 decoder 30, errors are detected by the 4 P parity bytes and short duration random errors are corrected. Larger errors, for example, long burst errors, may result in a number of C1 rows being uncorrectable or having two correctable errors. These rows will be appropriately flagged. For example, advanced decoders may mark each erroneous row using erasure flags in the expectation that the errors can be corrected at the C2 stage. All words found to be valid are passed along unprocessed. Thus, the C1 decoder 30 flags any errors identified, but not corrected, as indicated at 32. A C2 decoder 34 passes all words without flags as error free if they also appear error free during C2 decoding. The C2 decoder 34 attempts to correct any remaining errors using the Q parity values and any error flags.

As indicated, during decoding the C1 rows are examined first to detect isolated errors and apply correction. C1 decoders are usually set to correct at most a single arbitrary erroneous symbol and therefore are able to detect error conditions in excess of this limit accurately, and to pass along error detection information, in the form of flags, to the C2 decoder 34. At the C2 decoder, a detected error within the error-correction limits results in the correction of the errors. However, a detected error in excess of the error-correction limits results in the generation of a C2 flag as indicated. A C2 flag signifies that an uncorrectable error has been detected.

Figure 6 shows schematically an audio player. As can be seen, the data from a CD-DA 6 is passed to a *Red Book* decoder, indicated at 36, and then

may be fed directly to a sound reproduction device 38. However, where an uncorrectable error has been detected and a C2 flag generated, the data is fed via an error concealment unit 40 to the sound reproduction unit 38.

The nature of the error concealment unit 40 provided in an audio player varies and may, for example, incorporate sound muting circuits. In the illustrated embodiment, the error concealment unit 40 has been shown as an interpolator 40.

It will be appreciated that an audio waveform is generally continuous and that if an error produces a discontinuity in the waveform, the missing value can, in most cases be readily, and fairly accurately, be interpolated. However, where a data reader, for example, is being used to access digital data, interpolation cannot be used as the value of one symbol has no relationship to the symbol which is next retrieved. This provides a method of copy protecting CA-DAs, which copy protection scheme will allow play of a CD by an audio player whilst preventing the use of a data reader to make a useable copy of the disc.

Basically, for copy protection, unwanted noise is incorporated in the audio data recorded on the disc and is associated with error correction words which identify the unwanted noise as uncorrectable and thereby cause the generation of a C2 flag as described above. Such data will be passed by an audio player to an interpolator, as 40, which is able to remove the unwanted noise and substitute a more appropriate audio value. However, a data reader will simply read the audio data, flagged as uncorrectable, so that the unwanted noise is written to disc, for example, during copying. The copy disc, therefore, is significantly degraded.

A method of copy protecting CD-DAs by flagging introduced, unwanted noise on a disc as uncorrectable is proposed in WO 01/15028 and in GB0116278.3. These specifications propose altering the audio data by the addition of 'spikes' or superimposed impulses, and then changing the parity words associated with the C1 and C2 rows containing the changed audio data such that the altered audio data is identified, and flagged, as uncorrectable. Such spikes, if reproduced, are apparent as clicks in the audio output.

Generally, the scheme proposed in WO 01/15028 is to replace C2 parity bytes with unused symbols and to replace C1 parity bytes with zeros. In GB0116278.3 each codeword is changed by adding to at least part of a value thereof, a value representative of an uncorrectable error identifying syndrome.

With a copy protection scheme as proposed spikes are to be added to the audio data on a CD-DA to produce clicks. It is therefore important to ensure that all audio players are triggered to use their interpolators to remove the spikes no matter how sophisticated the decoder provided and irrespective of its methods of error correction. Clearly, the music industry will be unwilling to incorporate a copy protection technique if there is a realistic risk that the unwanted added noise will be audible when the consumer plays a genuine CD-DA on a typical consumer audio player.

However, with a copy protection scheme of this invention, the spikes or impulses which are added to the audio data can be controlled by reference to the audio data itself either to improve the playability or resultant audio which is reproduced, or to enhance the copy protection, or to provide some combination of these effects.

Thus, with the invention, one or more samples of the audio may be changed, as required. For example, this might be by the superimposition of impulses as described in WO 01/15028. All of the codewords which contain those altered samples are then identified and data in each of those codewords is changed to ensure that the codewords with the altered samples are reliably flagged as uncorrectable. This may be as set out in WO 01/15028. However, preferably, each codeword is changed by XORing bytes thereof with the coset leader value as described in GB0116278.3.

Figure 7 shows a system for copy protecting an audio compact disc. As is conventional, a *Red Book* encoder 50 receives incoming data for encoding and application, by way of a laser controller 52 and a recording laser 54, on to a master disc 60. Generally, the data fed to the *Red Book* encoder 50 will be audio data from a source 62. However, with the invention, the modifications to the data as discussed above are caused by the copy protection software which

is fed from a copy protection file source 64 to the *Red Book* encoder 50 in tandem with the audio data 62.

In WO 01/15028, audio data values are replaced with alternative values with random polarity. In this respect, Figure 8a shows an audio waveform, indicated at 80, and shows the application of various values 82 thereto. It will be appreciated that the loudness of the 'click' produced will vary according to the location of the altered value on the waveform 80.

With the present invention it is now proposed that at least some of the altered values should be located at a peak A on the audio waveform 80 as indicated in Figure 8b. This will have the result of maximising the loudness of the clicks and also ensures that the loudest passages of the audio data have the loudest clicks. Furthermore, the added value or spike superimposed on a peak as A should generally be of a large magnitude, but of the opposite polarity to the polarity of the peak as this provides a click which is most readily discernible to the human ear.

Thus, the use of superimposed impulses at or near peak values of the audio waveform, and with those superimposed impulses opposite in polarity to the polarity of the peak values, improves the effectiveness of the described method of copy protection.

The techniques illustrated in Figures 9 and 10 may be used alone or in conjunction with one or more of the techniques shown in Figures 8 to 10. In this respect, whereas the technique of Figure 8 enables the effectiveness of the copy protection method to be enhanced, the techniques shown in Figures 9 and 10 can be used either to increase the effectiveness of the copy protection method or to improve the audio output of an audio player. In this latter respect, it will be appreciated that the copy protection method of the invention requires the audio player to determine the existence of errors and then to conceal those errors, generally by use of an interpolator as 40 in Figure 6.

As indicated in Figure 9, during interpolation it is usual for the interpolator to use averages to calculate the replacement data for a sample which is flagged as erroneous. It will be appreciated that where the audio

waveform 80 is changing slowly and/or steadily, an interpolator will be able to calculate replacement data with much more accurate values than those calculated where there are large variations in individual values at a location along the waveform. For example, if a number of adjacent audio values are arranged along a straight line, the middle value 86 of a set of three values 84 to 88 can be determined with extreme accuracy.

Accordingly, it is proposed that additionally or alternatively to the provision of added values or spikes at peaks of the audio waveform 80, further of the added values or spikes should be incorporated at locations along the audio waveform 80 where the rate of change of the waveform is slow or the waveform is substantially linear. It will immediately be appreciated that, on playback, the interpolator will be able to replace such added values at such locations by accurate calculated values.

It is well known that time masking or frequency masking can be used, for example, to hide sounds from the human ear. The same effect can also be used to reveal added sound. In this respect, Figure 10 shows an audio waveform 80 applied to a filter 90 which divides it into 29 frequency sub-bands which are all audible to the human ear. If a superimposed impulse or spike 92 is applied at the peak value of each sub-band 94, as illustrated in Figure 10, its effect can be masked as far as the human ear is concerned. This is used where it is wished to minimise any degradation of the audio played from an original disc. Thus, for example, the clicks which are reproduced from added spikes can be masked by these known techniques so that they are not audible even if they are output in an audio player as correct audio samples rather than as error samples to be interpolated.

Where it is required to increase the effectiveness of the copy protection, the impulses as 92 shown in Figure 10 can be moved to occur at troughs in the individual frequency spectra rather than at the peaks whereby their existence on copied discs is particularly apparent.

It will be appreciated that variations and modifications may be made to the embodiment described and illustrated in accordance with the present invention.

CLAIMS

1. A method of copy protecting encoded, digital, audio data, the method comprising the steps of:

introducing altered values into the encoded digital audio data, and

changing all codewords containing the introduced altered values such that, on decoding, the codewords can be identified as uncorrectable,

wherein said altered values correspond to impulses superimposed onto the analog audio data, each said superimposed impulse being located at or near a peak in the analog audio waveform.

2. A method as claimed in Claim 1, wherein the impulses superimposed onto the analog audio data each have a polarity which is opposite to the polarity of the peak at or near which the superimposed impulse is located.

3. A method as claimed in Claim 1 or Claim 2, wherein the codewords are changed by modifying elements of the appropriate codewords.

4. A method as claimed in Claim 3, wherein at least four bytes of each codeword are changed by XOR with a value of four or more bytes.

5. A method as claimed in Claim 4, wherein all bytes changed are parity values.

6. A method as claimed in any preceding claim for use with an audio player provided with error concealment means, the method comprising the steps of arranging to identify codewords with altered values as uncorrectable, and forcing the altered data values to be subject to interpolation or other concealment techniques during playback of the audio data.

7. A method as claimed in any preceding claim, wherein the altered values are introduced by identifying peaks in the analog audio data and superimposing impulses on the analog audio data prior to its encoding.

8. A method as claimed in any of Claims 1 to 6, wherein the altered values are made in digital audio data at locations identified as peaks in the analog audio data.

9. A method as claimed in any preceding claim, wherein additional altered values correspond to impulses superimposed onto the analog audio data, each said additional superimposed impulse being located in the analog audio data where the audio waveform has a slow or steady rate of change.

10. A method of copy protecting encoded, digital, audio data, the method comprising the steps of:

introducing altered values into the encoded digital audio data, and

changing all codewords containing the introduced altered values such that, on decoding, the codewords can be identified as uncorrectable,

wherein said altered values correspond to impulses superimposed onto the analog audio data, each said superimposed impulse being located in the analog audio waveform where that audio waveform has a slow or steady rate of change.

11. A method as claimed in Claim 10, wherein an area in the analog audio waveform is located where there are at least three successive audio values arranged substantially in a straight line, and the superimposed impulse is located at a middle one of the three successive values.

12. A method as claimed in any preceding claim, wherein further additional altered values are introduced into the encoded digital audio data, said further additional altered values corresponding to impulses superimposed onto the analog audio waveform, the position of each said superimposed impulse being chosen after determining by time masking or frequency masking techniques whether or not it can be heard by the human ear.

13. A method of copy protecting encoded, digital, audio data, the method comprising the steps of:

introducing altered values into the encoded digital audio data, and

changing all codewords containing the introduced altered values such that, on decoding, the codewords can be identified as uncorrectable,

wherein said altered values correspond to impulses superimposed onto the analog audio waveform, each said superimposed impulse being located in the analog audio waveform as determined by frequency or time masking techniques.

14. A medium on which copy protected encoded digital audio data has been stored, wherein the medium carries digital audio data into which altered values have been introduced, and codewords, containing the introduced altered values, which have been changed such that they will be identified as uncorrectable on decoding, wherein said altered values correspond to impulses superimposed onto the analog audio data, the location of said superimposed impulses having been chosen by reference to the shape of the analog audio waveform.

15. A copy protection file arranged to alter digital audio data, and codewords produced therefrom, by methods as claimed in any of Claims 1 to 13.

16. A method of copy protecting encoded, digital, audio data, substantially as hereinbefore described with reference to the accompanying drawings.

17. A medium on which copy protected encoded digital audio data has been stored substantially as hereinbefore described with reference to the accompanying drawings.

18. A copy protection file arranged to alter digital audio data, and codewords produced therefrom, substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

INVESTOR IN PEOPLE

17

Application No:	GB 0118161.9	**Examiner:**	Paul Jefferies
Claims searched:	1-18	**Date of search:**	27 March 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
X	1, 3, 4, 6-11, 14-17	GB 2371916 A	(TTR TECHNOLOGIES) See figures 9, 10; page 22, lines 19-24 and page 24, lines 9-25.
X	1, 3, 4, 6-11, 14-17	WO 01/15028 A1	(TTR TECHNOLOGIES) See e.g. page 17, figures 9, 10 and page 23 particularly lines 24-31.
A		GB 2377511 A	(MACROVISION) See e.g. abstract, pages 3-4 and figures 1b, 5.
A, E		EP 1271511 A2	(MATSUSHITA) See whole document.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{V}:

G4A, G5R

Worldwide search of patent documents classified in the following areas of the IPC^{7}:

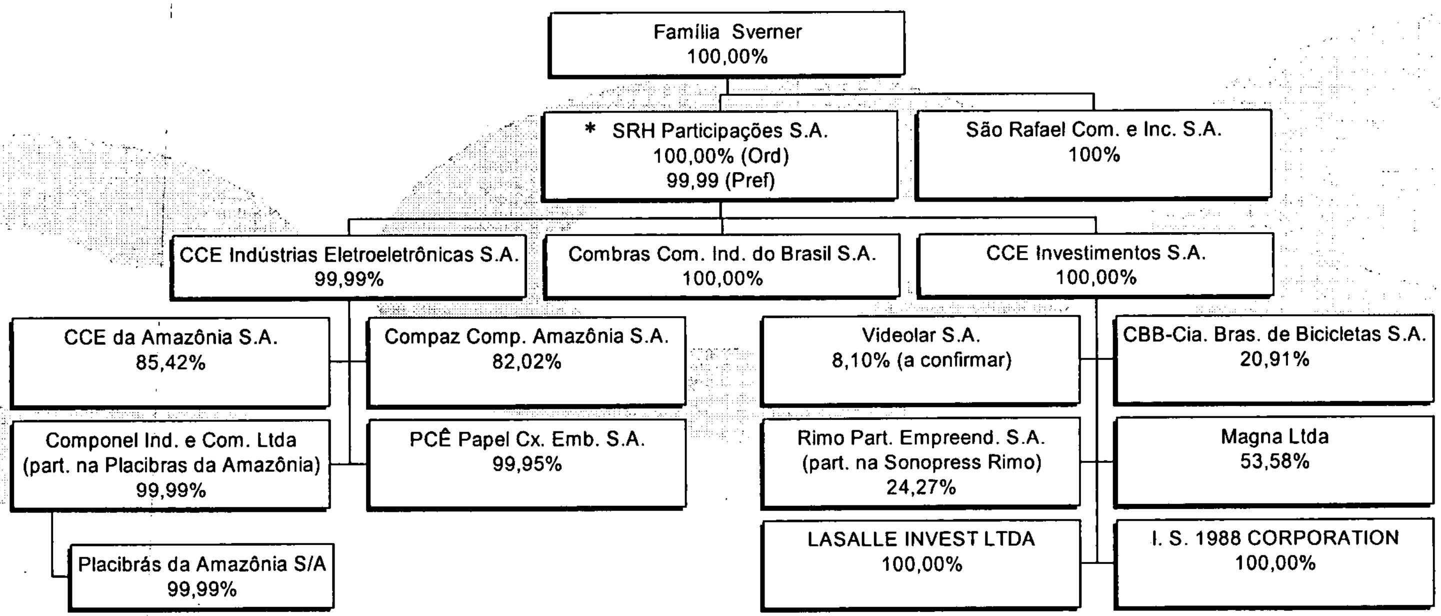
G06F

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, JAPIO, TDB, INSPEC

THIS PAGE BLANK (USPTO)

Grupo CCE: Estrutura Societária Simplificada Ago-2004



* Cisão da São Rafael em 31-dez-2003